

Table of Contents

In Memoriam: Steven R. Gilford	v
About the Contributors	vii
Table of Chapters	xix
Preface to the First Edition	lxi
Preface to the Second Edition	lxiii
Introduction	lxv

Chapter 1 A Brief History of Information Privacy Law

Daniel J. Solove

§ 1:1	Introduction	1-3
§ 1:2	Colonial America.....	1-4
§ 1:3	The Nineteenth Century	1-5
§ 1:3.1	New Threats to Privacy.....	1-5
[A]	The Census and Government Records.....	1-6
[B]	The Mail.....	1-6
[C]	Telegraph Communications.....	1-7
§ 1:3.2	The Fourth and Fifth Amendments	1-8
§ 1:3.3	Privacy of the Body	1-9
§ 1:3.4	Warren and Brandeis’s “The Right to Privacy”	1-10
§ 1:4	The Twentieth Century	1-12
§ 1:4.1	1900 to 1960	1-12
[A]	Warren and Brandeis’s Privacy Torts	1-12
[A][1]	Early Recognition	1-12
[A][2]	William Prosser and the <i>Restatement</i>	1-13
[A][2][a]	Intrusion upon Seclusion	1-13
[A][2][b]	Public Disclosure of Private Facts	1-14
[A][2][c]	False Light.....	1-15
[A][2][d]	Appropriation.....	1-15
[B]	The Emergence of the Breach of Confidentiality Tort.....	1-16
[C]	The Growth of Government Record Systems.....	1-17
[D]	The Telephone and Wiretapping	1-17
[D][1]	The Fourth Amendment: <i>Olmstead v.</i> <i>United States</i>	1-17

	[D][2]	Federal Communications Act Section 605.....	1-18
	[E]	The FBI and Increasing Domestic Surveillance.....	1-19
	[F]	Freedom of Association and the McCarthy Era	1-19
§ 1:4.2		The 1960s and 1970s	1-21
	[A]	New Limits on Government Surveillance	1-21
	[A][1]	Fourth Amendment Resurgence: <i>Katz v. United States</i>	1-21
	[A][2]	Title III of the Omnibus Crime and Control Act of 1968.....	1-21
	[B]	The Constitutional Right to Privacy	1-22
	[B][1]	Decisional Privacy: <i>Griswold v. Connecticut</i>	1-22
	[B][2]	Information Privacy: <i>Whalen v. Roe</i>	1-22
	[C]	Responses to the Rise of the Computer	1-22
	[C][1]	Burgeoning Interest in Privacy.....	1-22
	[C][2]	Freedom of Information Act of 1966	1-23
	[C][3]	Fair Information Practices	1-23
	[C][4]	Privacy Act of 1974	1-24
	[C][5]	Family Educational Rights and Privacy Act of 1974.....	1-25
	[C][6]	Foreign Intelligence Surveillance Act of 1978	1-26
	[D]	Financial Privacy.....	1-26
	[D][1]	Fair Credit Reporting Act of 1970.....	1-26
	[D][2]	Bank Secrecy Act of 1970	1-27
	[D][3]	<i>United States v. Miller</i>	1-28
	[D][4]	Right to Financial Privacy Act of 1978	1-28
	[E]	The Retreat from <i>Boyd</i>	1-29
	[F]	The Narrowing of the Fourth Amendment	1-29
§ 1:4.3		The 1980s	1-30
	[A]	Receding Fourth Amendment Protection	1-30
	[B]	The Growth of Federal Privacy Statutory Protection	1-31
	[B][1]	Privacy Protection Act of 1980	1-31
	[B][2]	Cable Communications Policy Act of 1984.....	1-31
	[B][3]	Computer Matching and Privacy Protection Act of 1988.....	1-31
	[B][4]	Employee Polygraph Protection Act of 1988	1-32
	[B][5]	Video Privacy Protection Act of 1988.....	1-32
	[C]	Electronic Communications Privacy Act of 1986.....	1-32
	[D]	OECD Guidelines and International Privacy	1-33
§ 1:4.4		The 1990s	1-34
	[A]	The Internet, Computer Databases, and Privacy	1-34
	[B]	The Continued Growth of Federal Statutory Protection	1-35
	[B][1]	Telephone Consumer Protection Act of 1991	1-35

Table of Contents

	[B][2]	Driver’s Privacy Protection Act of 1994.....	1-35
	[B][3]	Health Insurance Portability and Accountability Act of 1996.....	1-36
	[B][4]	Children’s Online Privacy Protection Act of 1998.....	1-37
	[B][5]	The Gramm-Leach-Bliley Act of 1999.....	1-37
	[C]	Beginning of FTC Section 5 Enforcement.....	1-38
	[D]	The EU Data Protection Directive.....	1-38
§ 1:5		The Twenty-First Century.....	1-39
	§ 1:5.1	After September 11: Privacy in a World of Terror.....	1-39
		[A] The USA PATRIOT Act of 2001.....	1-39
		[B] The FISA “Wall”.....	1-40
		[C] The Homeland Security Act of 2002.....	1-41
		[D] The Real ID Act of 2005.....	1-41
		[E] NSA Warrantless Surveillance; Edward Snowden Revelations.....	1-42
	§ 1:5.2	New Directions in Fourth Amendment Jurisprudence.....	1-42
	§ 1:5.3	Expansion of Consumer Privacy Protections.....	1-43
		[A] The Rise of the Privacy Profession and the Chief Privacy Officer.....	1-43
		[B] The Fair and Accurate Credit Transactions Act of 2003.....	1-43
		[C] The National Do-Not-Call Registry.....	1-44
		[D] The CAN-SPAM Act of 2003.....	1-44
		[E] Tort Law.....	1-44
		[F] Privacy Policies and Contract Law.....	1-45
		[G] FTC Enforcement.....	1-45
		[H] FCC Enforcement.....	1-46
		[I] The First Amendment and Privacy Law.....	1-46
	§ 1:5.4	The Rise of Data Security Law.....	1-47
	§ 1:5.5	The Launch and Evolution of HIPAA.....	1-48
	§ 1:5.6	Education Privacy Comes of Age.....	1-48
	§ 1:5.7	International Privacy Law.....	1-49
		[A] Asia-Pacific Economic Cooperation (APEC) Privacy Framework of 2004.....	1-49
		[B] International Data Protection Laws.....	1-49
		[C] Canada’s Anti-Spam Legislation (CASL).....	1-50
		[D] The Right to Be Forgotten.....	1-50
		[E] The Sinking of Safe Harbor.....	1-50
		[F] The General Data Protection Regulation (GDPR)....	1-50
§ 1:6		Conclusion.....	1-51

Chapter 2 Financial Privacy Law

Laura E. Goldsmith

§ 2:1 Summary and Introduction 2-4

 § 2:1.1 Evolution of Financial Privacy Law Parallels
 Developments in Computing..... 2-4

§ 2:2 Fair Credit Reporting Act and the Fair and Accurate
Credit Transactions Act 2-6

 § 2:2.1 Purpose and Background of the Fair Credit
 Reporting Act..... 2-6

 § 2:2.2 Coverage Under the FCRA..... 2-7

 [A] Definition of “Consumer” Under the FCRA..... 2-7

 [B] Definition of “Consumer Report” Under
 the FCRA..... 2-8

 [C] Definition of “Consumer Reporting Agency”
 Under the FCRA..... 2-11

 § 2:2.3 Permissible Use and Disclosure of Consumer
 Reports: The Obligation to Protect Against
 Unauthorized Access or Use of Consumer
 Information 2-15

 § 2:2.4 General Procedural Requirements for CRAs
 Under the FCRA 2-18

 § 2:2.5 Procedural Requirements for CRAs When
 Preparing and Issuing Consumer Reports for
 Employment Purposes 2-19

 § 2:2.6 Notice and Disclosure Requirements for CRAs
 Under the FCRA 2-20

 § 2:2.7 Unique Obligations with Respect to
 Investigative Consumer Reports 2-21

 § 2:2.8 Obligations for Users of Consumer Reports
 Under the FCRA 2-22

 § 2:2.9 Obligations for Resellers of Consumer Reports
 Under the FCRA 2-24

 § 2:2.10 Consumer Rights Under the FCRA to Dispute
 Information Contained in Consumer Reports..... 2-25

 § 2:2.11 Security Requirements of the FCRA Pertaining
 to Consumer Fraud and Identity Theft 2-27

 [A] Fraud Alerts 2-27

 [B] Blocking Identity Theft Information..... 2-29

 [C] Truncation of Card Numbers..... 2-30

 § 2:2.12 Affiliate Marketing Limits Under FACTA 2-36

 [A] Opt-Out Requirements 2-36

 [B] Exceptions 2-38

 [C] Delivery of Opt-Out Notices..... 2-39

 [D] Reasonable Opportunity and Means to Opt Out..... 2-39

Table of Contents

[E]	Duration of Opt-Out	2-40
[F]	Model Forms and Safe Harbor	2-40
§ 2:2.13	FACTA's Identity Theft Red Flags and Notices of Address Discrepancy Rules.....	2-40
[A]	Identity Theft Red Flags.....	2-40
[B]	Scope of the Red Flags Rules	2-42
[C]	Examples of Red Flags.....	2-44
[D]	Change of Address Requests	2-46
[E]	Address Discrepancy Notices	2-47
§ 2:2.14	Preemption of State Law by the FCRA	2-48
§ 2:2.15	Penalties for Violations of or Noncompliance with the FCRA.....	2-51
§ 2:3	Right to Financial Privacy Act.....	2-52
§ 2:3.1	Purpose and History of the Right to Financial Privacy Act.....	2-52
§ 2:3.2	Procedural Operation of the RFPA	2-53
§ 2:3.3	Substantive Aspects of the RFPA.....	2-55
§ 2:3.4	Interplay with State Statutes	2-57
§ 2:4	Gramm-Leach-Bliley Act	2-58
§ 2:4.1	Purpose and History of the Gramm-Leach-Bliley Act.....	2-58
§ 2:4.2	Internal Procedures and Systems to Ensure Confidentiality of Information.....	2-59
§ 2:4.3	Financial Institution's Notice Obligations	2-68
§ 2:4.4	Required Substance of Notice.....	2-73
[A]	Parties Who Must Serve Customers with Notice.....	2-74
§ 2:4.5	Limitations on Disclosure.....	2-75
[A]	Customer Must Opt Out of Third-Party Disclosures	2-75
[B]	Exceptions to Opt-Out Requirement.....	2-76
§ 2:4.6	Enforcement of the GLBA's Privacy Provisions.....	2-77
§ 2:4.7	GLBA's Relationship to Other Laws	2-78
[A]	GLBA Does Not Preempt State Laws	2-78
[B]	GLBA's Relationship with Other Federal Privacy Statutes	2-80
§ 2:5	Wall Street Reform and Consumer Protection Act	2-81
§ 2:5.1	Purpose and Background of Wall Street Reform and Consumer Protection Act	2-81
§ 2:5.2	Scope of CFPB Authority.....	2-82
§ 2:5.3	Powers and Duties of the CFPB	2-84
[A]	Rulemaking Authority	2-84
[B]	Evaluation of Existing Standards.....	2-85
[C]	Regulation of Unfair, Deceptive, and Abusive Acts or Practices	2-85
[D]	Examination of Financial Industry Participants.....	2-86

§ 2:5.4	Enforcement Authority of the CFPB.....	2-86
§ 2:5.5	Challenges to CFPB’s Structure and Independence.....	2-88
§ 2:6	Bank Secrecy Act	2-88
§ 2:6.1	Purpose and Background of the Bank Secrecy Act.....	2-88
§ 2:6.2	BSA Requirements	2-89
[A]	Record Creation, Storage, and Access	2-90
[B]	Reports of Suspicious Transactions	2-91
§ 2:7	Freedom of Information Act	2-93
§ 2:7.1	Background and Overview of FOIA.....	2-93
§ 2:7.2	Procedural Aspects of FOIA	2-94
§ 2:7.3	Protection of Financial Information	2-96
[A]	Trade Secrets and Commercial or Financial Information.....	2-96
[B]	Files Whose Disclosure Would Constitute Unwarranted Invasion of Privacy.....	2-99
[C]	Regulation or Supervision of Financial Institutions	2-100
§ 2:8	Electronic Fund Transfers Act.....	2-101
§ 2:8.1	Scope and Application.....	2-101
§ 2:8.2	Disclosure Requirements Under EFTA and the Act’s Implementing Regulations	2-101
§ 2:8.3	Additional EFTA Requirements Relating to Pre-Authorized Fund Transfers.....	2-103
§ 2:9	Sarbanes-Oxley Act.....	2-104
§ 2:10	State Laws Governing Financial Privacy	2-105
§ 2:10.1	Introduction.....	2-105
§ 2:10.2	State Constitutional Provisions Protecting Financial Privacy.....	2-105
§ 2:10.3	Statutory Provisions Protecting Financial Privacy Under State Law	2-105
[A]	Statutes Specifically Addressing Financial Privacy.....	2-106
[B]	General Privacy Statutes Implicating Financial Privacy.....	2-108
[C]	Statutes Restricting Access to Employee Credit Reports.....	2-109
[D]	State Security Breach Notification Laws	2-109
[E]	State Laws Implicating Information Security.....	2-111
[F]	State Laws Protecting Against Financial Fraud and Identity Theft.....	2-112
§ 2:10.4	Common Law Theories Asserted with Regard to Financial Privacy.....	2-113
[A]	Implied Contract	2-113
[B]	General Negligence.....	2-114

Table of Contents

[C] Invasion of Privacy..... 2-114
[D] Defamation..... 2-114
Appendix 2A Model Form with No Opt-Out..... App. 2A-1
Appendix 2B Model Form with All Opt-Out.....App. 2B-1

Chapter 3 Medical Privacy

Ryan P. Blaney & Matthew J. Westbrook

§ 3:1 Introduction 3-3
§ 3:2 HIPAA Administrative Simplification 3-4
 § 3:2.1 Background 3-4
 § 3:2.2 Definitions..... 3-5
 § 3:2.3 HIPAA Privacy 3-7
 [A] Basic Rules..... 3-7
 [B] Limitations on Sale of PHI..... 3-8
 [C] Limitation on Use of PHI for Paid Marketing 3-9
 § 3:2.4 HIPAA Security: Basic Rules 3-10
 § 3:2.5 Business Associates 3-11
 § 3:2.6 HIPAA Security Breach Notification 3-12
 § 3:2.7 Sanctions for Violations of the Privacy and
 Security Rules 3-14
§ 3:3 State Law and HIPAA Privacy Preemption 3-24
§ 3:4 Heightened Protection for Specialized Types of
 Medical Information..... 3-25
 § 3:4.1 Communicable Diseases..... 3-25
 [A] HIV/AIDS..... 3-26
 [B] Confidentiality and Disclosure of HIV
 Test Results..... 3-27
 § 3:4.2 Authorized Disclosure..... 3-27
 § 3:4.3 Remedies for Breach of Confidentiality 3-28
 § 3:4.4 Sexually Transmitted Disease 3-32
 § 3:4.5 Tuberculosis..... 3-34
 § 3:4.6 Genetic Information 3-36
 [A] Genetic Discrimination 3-36
 [B] DNA Sampling by Law Enforcement 3-37
§ 3:5 Privacy of Substance Use Disorder Records 3-38
 § 3:5.1 Introduction..... 3-38
 § 3:5.2 Scope of Applicability..... 3-39
 § 3:5.3 Exceptions to Substance Use Disorder
 Confidentiality Laws..... 3-41
 § 3:5.4 Other Exceptions Permitting Information
 Release..... 3-42
 [A] Release with Patient’s Consent 3-42
 [B] Voluntary Disclosure to the Criminal
 Justice System..... 3-43

[C]	Release Without a Patient’s Consent	3-44
[D]	Releases Authorized by a Court Order	3-45
[E]	Request for Records in a Criminal Proceeding.....	3-46
[E][1]	Confidential Information	3-47
§ 3:5.5	Conclusion	3-49
§ 3:6	HIPAA Privacy and Security Considerations During and After a PHE.....	3-49
§ 3:6.1	Permissible Disclosures of PHI	3-50
§ 3:6.2	HHS’s Waiver of Sanctions and Penalties and OCR’s Enforcement Discretion	3-53
§ 3:6.3	Post-PHE Considerations.....	3-55
§ 3:7	Medical Privacy at Common Law	3-57
§ 3:7.1	Actions Arising Out of the Disclosure of Confidential Medical Information	3-57
[A]	Theory of Recovery	3-57
[B]	Exceptions to Liability	3-59
§ 3:7.2	The Duty to Warn.....	3-61
§ 3:8	Privilege.....	3-63
§ 3:8.1	State Law	3-64
[A]	Physician-Patient Privilege.....	3-64
[A][1]	Majority of States Have Enacted Privilege by Statute.....	3-64
[A][2]	Scope of the Privilege.....	3-64
[A][2][a]	Types of Providers Covered.....	3-64
[A][2][b]	Subject Matter of the Privilege.....	3-65
[A][2][c]	Who May Assert the Privilege	3-65
[A][2][d]	Waiver	3-66
[A][2][e]	Exceptions/Exemptions	3-66
[B]	Psychotherapist-Patient Privilege	3-67
[B][1]	Every State Has Enacted Privilege by Statute	3-67
[B][2]	Scope of the Privilege.....	3-68
[B][2][a]	Types of Providers Covered.....	3-68
[B][2][b]	Subject Matter of the Privilege.....	3-68
[B][2][c]	Who May Assert the Privilege	3-68
[B][2][d]	Waiver	3-69
[B][2][e]	Exceptions/Exemptions	3-69
§ 3:8.2	Federal Law.....	3-70
[A]	Psychiatrist-Patient Privilege.....	3-71
[A][1]	Rule.....	3-71
[A][2]	Waiver	3-71
[A][3]	Exceptions	3-72
[A][3][a]	The Dangerous-Patient Exception	3-72
[A][3][b]	The Crime-Fraud Exception	3-72
[A][3][c]	Other Exceptions.....	3-73
[B]	Physician-Patient Privilege.....	3-73

Table of Contents

[C]	Diversity and Supplemental Jurisdiction.....	3-74
[C][1]	Diversity Jurisdiction	3-74
[C][2]	Supplemental Jurisdiction	3-74
§ 3:9	Employers and Medical Privacy	3-75
§ 3:9.1	Americans with Disabilities Act	3-75
§ 3:9.2	HIPAA and Employer-Sponsored Health Plans.....	3-78
[A]	Overview of HIPAA Privacy Rules and Applicability to Health Plans	3-78
[B]	Sharing Information with Plan Sponsors Under HIPAA	3-79
§ 3:10	Technological Advancements and Recent Litigation Involving Sensitive Health Information.....	3-83
§ 3:10.1	Artificial Intelligence (AI).....	3-83
§ 3:10.2	Online Tracking Technologies	3-85
[A]	PHI	3-86
[B]	User-Authenticated Webpages.....	3-86
[C]	Unauthenticated Webpages.....	3-87
[D]	Mobile Apps	3-88
[E]	HIPAA Compliance Obligations.....	3-89
§ 3:10.3	Recent Class Action Litigation.....	3-90
§ 3:10.4	Recent FTC Enforcement Action	3-91

**Chapter 4 Federal Trade Commission Enforcement of
Privacy**

*David A. Munkittrick, Brooke Gottlieb &
Amy Gordon*

§ 4:1	The Federal Trade Commission.....	4-2
§ 4:2	Enforcement Tools Available to the Commission	4-3
§ 4:2.1	Overview.....	4-3
§ 4:2.2	Investigation	4-4
§ 4:2.3	Administrative Enforcement Action.....	4-4
§ 4:2.4	Judicial Enforcement.....	4-6
§ 4:3	Privacy and Security Promises and Policies	4-6
§ 4:3.1	Overview.....	4-6
§ 4:3.2	Authority	4-6
§ 4:3.3	Illustrative Enforcement Practice	4-8
§ 4:3.4	FTC Guidance	4-12
§ 4:4	Data Security and Identify Theft	4-12
§ 4:4.1	Authority	4-12
§ 4:4.2	Illustrative Enforcement Practice	4-12
§ 4:4.3	FTC Guidance	4-17
§ 4:5	Digital and Online Privacy.....	4-19
§ 4:5.1	Overview.....	4-19

§ 4:5.2	Spyware	4-19
§ 4:5.3	Big Data.....	4-21
§ 4:5.4	Behavioral Advertising	4-23
§ 4:5.5	Algorithms and Artificial Intelligence	4-27
§ 4:5.6	Overlap with Antitrust.....	4-29
§ 4:6	Children’s Privacy.....	4-32
§ 4:6.1	Authority	4-32
§ 4:6.2	Illustrative Enforcement Practice	4-35
§ 4:6.3	FTC Guidance	4-39
§ 4:7	Financial Privacy.....	4-41
§ 4:7.1	Authority	4-41
§ 4:7.2	Illustrative Enforcement Practice	4-45
§ 4:7.3	FTC Guidance	4-48
§ 4:8	International: The EU-U.S. Privacy Shield Framework.....	4-49
§ 4:8.1	Overview of the EU-U.S. Privacy Shield Framework.....	4-49
	[A] The <i>Schrems</i> Rulings.....	4-51
§ 4:8.2	Illustrative Enforcement Practice	4-54
§ 4:8.3	FTC Guidance	4-55

Chapter 5 State Privacy Laws

Ryan P. Blaney

§ 5:1	Introduction	5-3
§ 5:1.1	Overview: Role of State Governments.....	5-3
§ 5:1.2	Origins of State Privacy Laws.....	5-8
	[A] Judicial—Torts and Crimes.....	5-8
	[B] Constitutional	5-9
	[C] Statutory.....	5-11
	[C][1] The California Invasion of Privacy Standard	5-13
§ 5:2	Online Privacy	5-15
§ 5:2.1	State Online Privacy Protection Statutes.....	5-15
	[A] California Online Privacy Protection Act (CalOPPA)	5-15
	[B] Online Privacy Laws in Other States.....	5-18
	[C] Related State Legislation Affecting Online Businesses	5-21
§ 5:2.2	Employee Social Media Protection Laws	5-22
§ 5:2.3	Revenge Porn Laws	5-23
§ 5:2.4	State Student Data Privacy Legislation.....	5-24
§ 5:2.5	Children’s Privacy and Social Media	5-26
§ 5:3	Florida’s Digital Bill of Rights.....	5-29

Table of Contents

§ 5:4	Spyware	5-30
§ 5:4.1	California.....	5-31
§ 5:4.2	Other States Following California's Approach.....	5-32
§ 5:4.3	Other States with More Limited Spyware Statutes.....	5-34
§ 5:5	Exposure of Personal Identifying Information.....	5-35
§ 5:5.1	Laws Criminalizing Identity Theft.....	5-35
§ 5:5.2	Laws Allowing Victims to Initiate Investigations and/or Clear Their Names	5-37
§ 5:5.3	Rights of Action Against Perpetrators	5-38
§ 5:5.4	Protections and Rights of Action Against Debt Collectors	5-38
§ 5:5.5	Notice of Security Breach Legislation.....	5-39
[A]	The California Framework.....	5-41
[B]	Other State Security Breach Notification Provisions	5-45
[B][1]	“Material” Breach Necessary to Trigger Notification.....	5-45
[B][2]	Expanded Definition of “Personal Information”	5-48
[B][3]	Necessity to Notify Customers of a Breach of Non-Computerized Data.....	5-52
[B][4]	Notification Procedures	5-53
[B][5]	Duty to Notify Other Entities	5-58
[B][6]	Duty of Non-Owners Maintaining Data	5-61
[B][7]	Exemption from Notification for Entities in Compliance with GLBA	5-62
[B][8]	Exemption from Notification for Encrypted Information.....	5-63
[B][9]	Penalties for Violation	5-65
[B][10]	Laws Requiring Reimbursement of Card-Issuing Financial Institutions for Costs Associated with a Data Breach	5-69
[B][11]	Credit Freeze Laws	5-70
§ 5:5.6	Data Security and Destruction Requirements	5-72
§ 5:5.7	Consumer Data Privacy Legislation	5-74
[A]	The California Consumer Privacy Act of 2018	5-75
[A][1]	Covered Businesses and Preemption	5-76
[A][2]	Definition of “Selling”	5-76
[A][3]	Consumer Rights and Covered Business Obligations.....	5-77
[A][4]	Enforcement and Private Right of Action	5-79
[B]	The California Privacy Rights Act of 2020.....	5-80
§ 5:6	Financial Privacy.....	5-81
§ 5:6.1	California Financial Information Privacy Act.....	5-81
§ 5:6.2	New York Cybersecurity Regulation.....	5-82
§ 5:6.3	Other States.....	5-83

§ 5:6.4	Preemption	5-84
§ 5:6.5	Credit Card Transactions	5-85
[A]	Restrictions on Merchants	5-85
[B]	Prohibition on Disclosure of Marketing Information	5-88
§ 5:7	Privacy of Insurance-Related Information	5-89
§ 5:7.1	The National Association of Insurance Commissioners (NAIC) Model Acts	5-89
§ 5:7.2	Definitions of “Personal Information” and Similar Terms	5-92
§ 5:7.3	The GLBA Joint Marketing Exception and 2002 Model Act States	5-93
§ 5:8	Laws Governing Disclosure and Use of Social Security Numbers	5-93
§ 5:8.1	The California Framework	5-95
[A]	Jurisdictional Divergence from the California Framework	5-97
[A][1]	Prohibiting SSNs in Customer Mailings	5-97
[A][2]	Expanded Exemptions from the California Framework	5-97
§ 5:8.2	Other State Law Regulation of the Use of Social Security Numbers	5-99
[A]	Requiring a Consumer’s SSN to Complete a Transaction	5-99
[B]	Privacy Policy for Handling SSNs	5-100
[C]	Employers	5-101
[D]	Other Variations on the California Framework	5-102
§ 5:9	Unsolicited Telephone Marketing	5-102
§ 5:9.1	Telemarketing: State Do-Not-Call Laws	5-102
§ 5:9.2	Laws Restricting Cell Phone Marketing	5-105
§ 5:10	Spam	5-106
§ 5:10.1	The Federal Statute and Preemption	5-107
§ 5:10.2	State Regulation of Spam	5-111
[A]	Opt-In Provisions	5-111
[B]	Opt-Out Provisions	5-112
[C]	Subject-Line Labeling Requirements	5-112
[D]	Provisions Prohibiting False or Misleading Practices	5-112
[E]	Bans on Selling Software That Can Be Used to Falsify Routing Information	5-114
§ 5:11	Electronic Surveillance	5-114
§ 5:11.1	State Statutory Schemes	5-114
§ 5:12	Radio Frequency Identification and Location Tracking	5-117

Table of Contents

§ 5:13 Biometric Privacy Laws..... 5-120
 § 5:13.1 The Illinois Framework..... 5-121
 § 5:13.2 The Washington Framework..... 5-124
 § 5:13.3 The Colorado Framework..... 5-126

Chapter 6 Privacy of Electronic Communications

Bruce Boyden

§ 6:1 Introduction 6-2
 § 6:1.1 Purpose and History of the ECPA 6-4
 § 6:1.2 Amendments to the ECPA..... 6-9
§ 6:2 Title I—The Wiretap Act 6-10
 § 6:2.1 Communications Covered 6-12
 [A] Oral Communications..... 6-13
 [A][1] Expectation of Privacy 6-13
 [A][2] Silent Video 6-20
 [B] Wire Communications 6-21
 [B][1] Cordless Phones 6-22
 [B][2] Voice Mail 6-24
 [C] Electronic Communications 6-25
 § 6:2.2 Intentional Interception of Communications 6-27
 [A] “Intercept” 6-27
 [A][1] Contemporaneous Acquisition Requirement..... 6-28
 [A][2] Access to Temporarily Stored Emails 6-33
 [A][3] Access to Telephone Numbers or Other
 Associated Information 6-42
 [A][4] Keyloggers and Screen Captures 6-45
 [B] Intent..... 6-48
 § 6:2.3 Use or Disclosure of an Intercepted
 Communication 6-51
 § 6:2.4 Exceptions 6-55
 [A] Communications Service in Normal Course of
 Business..... 6-55
 [B] Consent by a Party to a Communication 6-60
 [B][1] Implied Consent..... 6-66
 [B][2] Tortious or Criminal Purpose Exception..... 6-68
 [B][3] The Case of “Cookies” 6-70
Figure 6-1 Placing Third-Party Advertisements on
 a Website 6-71
 [C] Business Extensions..... 6-74
 [D] Communications to the Public..... 6-80
 [E] First Amendment 6-82
 § 6:2.5 Private Cause of Action..... 6-86
 [A] Litigating Wiretap Act Claims 6-89
 [B] Limitations 6-95

[C]	Damages.....	6-97
[D]	Good-Faith Defense.....	6-100
§ 6:2.6	State Wiretap Acts.....	6-102
§ 6:3	Title II—Stored Communications Act.....	6-104
§ 6:3.1	Access to Stored Communications.....	6-105
[A]	Electronic Communication Service Facility.....	6-106
[B]	“Unauthorized Access”.....	6-111
[B][1]	Privacy Policies.....	6-114
[B][2]	Subpoenas.....	6-115
[B][3]	Exceeding Authorized Access.....	6-117
[C]	“Electronic Storage”.....	6-118
[C][1]	Cookies and Other Data Stored on Computers.....	6-121
[D]	Exceptions.....	6-122
[D][1]	Access Authorized by a Service Provider.....	6-123
[D][2]	Access Authorized by a Party.....	6-123
§ 6:3.2	Disclosures by Communications Services.....	6-126
[A]	Disclosures Prohibited Under Section 2702.....	6-126
[A][1]	Contents of Communications.....	6-130
[A][1][a]	Exceptions.....	6-131
[A][2]	Customer Records.....	6-137
[A][2][a]	Exceptions.....	6-139
[A][3]	Anti-Pretexting Laws.....	6-140
[B]	Disclosures to the Government Required Under Section 2703.....	6-142
§ 6:3.3	Private Cause of Action.....	6-145
[A]	Damages.....	6-148
§ 6:4	Title III—Pen Registers and Trap-and-Trace Devices.....	6-149

Chapter 7 **The Foreign Intelligence Surveillance Act**

Mary Edquist & Brian Morrison

§ 7:1	Introduction.....	7-2
§ 7:1.1	Purpose.....	7-3
§ 7:1.2	“Special-Needs” Exception to Warrant Requirement.....	7-3
§ 7:1.3	Evolution of FISA.....	7-4
[A]	The Church Committee.....	7-5
[B]	Amendments to FISA.....	7-6
§ 7:2	The Foreign Intelligence Surveillance Act.....	7-7
§ 7:2.1	The Scope of FISA.....	7-7
[A]	Intelligence-Gathering Activities Targeting Persons Within the United States.....	7-7
[B]	Intelligence-Gathering Activities Targeting Persons Outside the United States.....	7-10

Table of Contents

§ 7:2.2	Required Elements for Authorized Intelligence-Gathering Pursuant to FISA	7-11
[A]	Probable Cause	7-11
[B]	Significant Purpose	7-13
[C]	Identification and Description of the Targeted Individual, Facility, Place, or Property	7-14
[D]	Target Is a Foreign Power or an Agent of a Foreign Power	7-16
[E]	The Method and Time Frame of Intelligence Collection	7-18
[F]	Minimization Procedures.....	7-20
[G]	Certification Requirements.....	7-21
§ 7:2.3	Exceptions to FISA Authorization or Order Requirement	7-23
[A]	Surveillance of Certain Foreign Powers	7-23
[B]	During Emergencies While FISC Order Is Being Pursued	7-25
[C]	Declaration of War	7-28
[D]	Testing of Equipment	7-28
[E]	Discovery of Unauthorized Surveillance Equipment	7-29
[F]	Training	7-29
§ 7:2.4	Remedies	7-30
[A]	Motion to Suppress.....	7-30
[B]	Request to Modify or Set Aside Order	7-32
[C]	Civil Liability.....	7-33
[D]	Criminal Liability	7-35
§ 7:3	The Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review	7-35
§ 7:3.1	Membership and Structure	7-35
§ 7:3.2	Authority, Jurisdiction, and Scope of Review	7-36
§ 7:3.3	Secret/Sensitive Nature of FISC and FISCRC Matters	7-37
[A]	Secrecy of Proceedings	7-37
[B]	Publication of Opinions	7-38
[C]	Disclosure and Reporting Requirements; Measures to Increase Transparency.....	7-41
§ 7:3.4	Procedure for Obtaining a FISC Order	7-42
§ 7:4	Controversies and Amendments.....	7-46
§ 7:4.1	The Terrorist Surveillance Program and Retroactive Immunity	7-46
§ 7:4.2	Targeting U.S. and Non-U.S. Persons Abroad	7-48
[A]	Bulk Collection of Telephonic Metadata	7-49
[B]	PRISM and the Collection of Internet Communications in Transit.....	7-50

§ 7:4.3 Expansion of the Business Records Provision..... 7-53
 § 7:4.4 Roving Wiretaps..... 7-54
 § 7:4.5 Lone Wolf Provision..... 7-55

Chapter 8 Privacy and Homeland Security

Hugo Teufel III

§ 8:1 Background: Intelligence, Surveillance, and Privacy Pre-9/11 8-2
 § 8:2 Establishment of Department of Homeland Security..... 8-4
 § 8:2.1 DHS Organization and Functions 8-5
 § 8:2.2 Authorities for Privacy Protection at DHS..... 8-6
 Figure 8-1 DHS Organization Chart 8-8
 § 8:3 Privacy Protection at Other Agencies 8-9
 § 8:3.1 Internal Privacy Protection Requirements for Executive-Branch Agencies 8-9
 § 8:3.2 Executive-Branch Privacy/Civil Liberties Oversight 8-13
 [A] Board on Safeguarding Americans' Civil Liberties 8-13
 [B] Privacy and Civil Liberties Oversight Board 8-14
 § 8:4 DHS Privacy Office Functions 8-18
 § 8:4.1 Policy 8-19
 [A] Fair Information Practice Principles..... 8-19
 [B] Use of Social Media 8-21
 [C] Extending Privacy Act Protections..... 8-22
 [D] Other Guidance 8-24
 § 8:4.2 Compliance 8-24
 § 8:4.3 Oversight 8-26
 § 8:4.4 Incidents and Breaches 8-29
 § 8:4.5 Education and Training..... 8-30
 § 8:4.6 Outreach..... 8-33
 § 8:5 High-Profile Privacy Issues in Homeland Security 8-34
 § 8:5.1 Information-Sharing 8-34
 [A] Breaking Down the Wall of Separation..... 8-34
 [B] Information Sharing Environment (ISE) 8-35
 § 8:5.2 Fusion Centers..... 8-38
 [A] Organization and Mission 8-38
 [B] Civil Liberties Concerns 8-41
 § 8:5.3 Watchlists 8-43
 [A] Watchlists, Pre-9/11 8-43
 [B] Integration and Use of Screening Information 8-44
 [C] Redress and Oversight 8-45
 § 8:5.4 Data Mining 8-47
 [A] Privacy Concerns Versus Combating Terrorism..... 8-47
 [B] Establishing a Uniform Definition of "Data Mining" 8-48

Table of Contents

[C]	High-Profile Data Mining	8-52
[C][1]	Program “Able Danger”	8-53
[C][2]	JetBlue Data Transfer	8-54
[C][3]	Total Information Awareness/Terrorism Information Awareness (TIA).....	8-54
[C][4]	Multistate Anti-Terrorism Information Exchange (MATRIX).....	8-56
[C][5]	Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE)....	8-56
§ 8:5.5	Transatlantic Exchanges of Personal Data.....	8-57
[A]	Background.....	8-57
[B]	Conflicting Data-Protection Requirements	8-58
[C]	Common Principles Underlying Future Information-Sharing	8-60

Chapter 9 Workplace Privacy Law

Kathleen M. McKenna & Anthony J. Oncidi

§ 9:1	Selection of Employees	9-4
§ 9:1.1	Pre-Employment Inquiries	9-4
[A]	Inquiries Regarding Race, Sex, Religion, and Other Protected Characteristics	9-4
[B]	Disability-Related Inquiries	9-7
[C]	Psychological Testing and Examinations.....	9-8
[D]	Union Status	9-9
[E]	Litigation History	9-9
[F]	Social Media	9-10
[G]	Salary History.....	9-10
§ 9:1.2	References.....	9-12
§ 9:1.3	Blacklisting.....	9-15
§ 9:2	Collection of Personal Information.....	9-16
§ 9:2.1	Medical Information.....	9-18
[A]	Pandemics.....	9-18
[B]	Health Insurance Portability and Accountability Act of 1996.....	9-18
[C]	HIV/AIDS.....	9-21
[D]	Confidentiality of Patient Medical Records	9-23
[D][1]	Federal Law	9-23
[D][2]	State Law.....	9-24
[E]	Employee Wellness Programs.....	9-29
§ 9:2.2	Past Criminal and Arrest Records	9-30
[A]	Federal Law.....	9-30
[A][1]	Title VII	9-30
[A][2]	Intelligence Reform and Terrorism Prevention Act.....	9-34

	[B]	State and Local Law	9-35
	[B][1]	Generally.....	9-35
	[B][2]	“Ban-the-Box” Laws	9-37
§ 9:2.3		Fingerprints and Photographs	9-40
§ 9:2.4		Financial Data	9-42
	[A]	Federal Law.....	9-42
	[A][1]	Fair Credit Reporting Act of 1970.....	9-42
	[A][2]	Fair and Accurate Credit Transactions Act	9-44
	[B]	State Law	9-44
§ 9:2.5		Educational Records.....	9-46
	[A]	Federal Law.....	9-46
	[B]	State Law	9-47
§ 9:2.6		Personal Identification Information	9-48
	[A]	Information Stored on Computers	9-48
	[B]	Social Security Numbers.....	9-49
	[C]	Motor Vehicle Information	9-51
	[D]	Verification of Employment Eligibility: E-Verify.....	9-53
§ 9:2.7		Access to Personnel Records.....	9-54
§ 9:2.8		Genetic Information	9-57
§ 9:2.9		Biometric Information	9-58
§ 9:3		Policies Regulating Employee Conduct	9-59
§ 9:3.1		Sexual Conduct, Intimate Relationships, Fraternization, Procreation, Marriage.....	9-59
	[A]	Common-Law Claims—Private Employees	9-59
	[A][1]	Invasion of Privacy	9-59
	[A][1][a]	Public Disclosure of Private Facts.....	9-59
	[A][1][b]	Intrusion upon Seclusion	9-61
	[A][2]	Wrongful Termination in Violation of Public Policy.....	9-63
	[B]	Statutory Claims	9-64
	[C]	Constitutional Privacy Right.....	9-64
§ 9:3.2		Grooming and Dress Codes	9-67
	[A]	Mutable Versus Immutable Characteristics	9-67
	[B]	Hair Length and Style	9-69
	[B][1]	Federal Law	9-69
	[B][2]	State Law.....	9-72
	[C]	Beards and Moustaches	9-73
	[C][1]	Federal Law	9-73
	[C][2]	State Law.....	9-75
	[D]	Dress Codes.....	9-75
	[D][1]	Federal Law	9-75
	[D][2]	State Law.....	9-77
	[E]	Gender Identity/Expression Issues	9-78
	[E][1]	Federal Law	9-78
	[E][2]	State Law.....	9-79

Table of Contents

§ 9:3.3	Polygraphs and Lie Detector Tests.....	9-81
§ 9:3.4	Genetic Testing.....	9-83
§ 9:3.5	Drug and Alcohol Use	9-84
[A]	Federal Law.....	9-85
[A][1]	Constitution.....	9-85
[A][2]	Americans with Disabilities Act (ADA).....	9-86
[A][3]	Other Federal Statutes and Regulations.....	9-88
[B]	State Laws.....	9-89
[B][1]	Constitutions	9-89
[B][2]	Statutes	9-90
[C]	Medical Marijuana in the Workplace	9-91
[D]	Contractual and Common Law Theories of Liability	9-94
§ 9:3.6	Smoking.....	9-95
[A]	Restrictions on Smoking in the Workplace	9-95
[B]	Off-Duty Smoking	9-97
§ 9:3.7	Disclosure of Wages	9-98
[A]	Federal Law.....	9-98
[B]	State Law	9-99
§ 9:3.8	Blogging and Cybersmearing.....	9-101
[A]	Validity of Employee Confidentiality Policies	9-101
[B]	Potential Causes of Action.....	9-105
[B][1]	Private Blogs and the Stored Communications Act	9-105
[B][2]	Trespass to Chattels	9-107
[B][3]	Defamation	9-108
§ 9:4	Surveillance of Employees.....	9-110
§ 9:4.1	Employer Investigations Generally.....	9-110
§ 9:4.2	Physical Searches	9-110
[A]	Introduction	9-110
[B]	Public Employer Searches	9-111
[C]	Private Employer Searches	9-114
[C][1]	Third-Party Consent	9-116
[C][2]	Fifth Amendment Considerations	9-116
[D]	National Labor Relations Act.....	9-117
§ 9:4.3	Email and Internet Use Searches	9-118
[A]	Notice.....	9-118
[B]	Statutory Provisions.....	9-122
[B][1]	Federal Law	9-122
[B][1][a]	The Electronic Communications Privacy Act	9-122
[B][1][a][i]	Exceptions	9-125
[B][1][b]	The Federal Computer Fraud and Abuse Act.....	9-127
[B][1][c]	National Labor Relations Act	9-131
[C]	State Law	9-132

§ 9:4.4	Instant Electronic Communications	9-134
[A]	Instant Messaging.....	9-134
[B]	Text Messaging	9-135
[C]	Social Media	9-136
§ 9:4.5	Eavesdropping, Recording Telephone Conversations, and Video Monitoring	9-138
§ 9:4.6	Human Tracking Devices.....	9-142
[A]	Global Positioning Systems (GPS)	9-142
[B]	Radio Frequency Identification (RFID).....	9-145
[C]	Biometrics	9-146

Chapter 10 Privacy and Commercial Communications

Michael Hintze & Robert Forbes

§ 10:1	Overview	10-3
§ 10:1.1	Connection to Privacy Principles and Laws.....	10-3
§ 10:1.2	General Considerations	10-4
§ 10:2	Email Communications.....	10-5
§ 10:2.1	Source and Scope of Rules.....	10-5
§ 10:2.2	What Is a “Commercial Electronic Mail Message”?	10-7
§ 10:2.3	Who Is the “Sender”?.....	10-9
§ 10:2.4	Consent Requirements	10-12
§ 10:2.5	Information to Be Included in Each Message	10-13
§ 10:2.6	Forward-to-a-Friend Features	10-14
§ 10:2.7	Specific Rules for Messages Sent to Wireless Domains.....	10-16
§ 10:2.8	Prohibitions on Fraudulent, Deceptive, and Abusive Practices	10-18
§ 10:2.9	Additional Rules Regarding Sexually Oriented Material	10-19
§ 10:3	Telephone Communications.....	10-21
§ 10:3.1	Source and Scope of Rules.....	10-21
§ 10:3.2	Consent Requirements	10-22
[A]	Company-Specific Consent Requirements	10-22
[B]	National Do-Not-Call Registry	10-23
[C]	State Do-Not-Call Lists	10-25
§ 10:3.3	Required Call Content	10-26
§ 10:3.4	Time and Frequency Restrictions	10-28
§ 10:3.5	Use of Autodialers, Prerecorded Messages, and Other Technologies	10-28
§ 10:3.6	Prohibitions on Deceptive or Abusive Telemarketing Practices	10-32
§ 10:3.7	Record-Keeping and Compliance Requirements	10-33

Table of Contents

§ 10:4	Fax Communication.....	10-35
§ 10:4.1	Source and Scope of Rules.....	10-35
§ 10:4.2	Consent Requirements	10-35
§ 10:4.3	Information to Be Included in Each Message	10-37
§ 10:5	Direct Mail Communications.....	10-38
§ 10:5.1	Source and Scope of Rules.....	10-38
§ 10:5.2	Restrictions and Prohibitions on Mailing Certain Content.....	10-38
[A]	Fraudulent or Deceptive Content.....	10-39
[B]	Prohibited or Restricted Advertising Content.....	10-39
[C]	Mailings Containing Certain Goods, Samples, Etc	10-40
§ 10:5.3	Consent Requirements	10-41
[A]	Sexually Oriented Advertisements	10-41
[B]	“Pandering” Advertisements	10-42
[C]	Sweepstakes and Skill Contests	10-43
§ 10:6	Text Messaging.....	10-43
§ 10:6.1	Source and Scope of Rules.....	10-43
§ 10:6.2	What Is a Text Message?.....	10-43
§ 10:6.3	Consent Requirements	10-44
[A]	Messages Sent to a Number.....	10-44
[A][1]	Do-Not-Call Rules	10-45
[A][2]	Revocation of Consent or Opt-Out Requests	10-45
[B]	Messages Sent to a Username and Domain Name.....	10-46
[B][1]	Express Prior Authorization.....	10-47
[B][2]	FCC List of Wireless Domains	10-48
[B][3]	Procedures for Receiving and Honoring Opt-Out Requests	10-48
[C]	State-Law Consent Requirements	10-49
[C][1]	California	10-49
[C][2]	Rhode Island	10-51
[C][3]	Washington	10-52
[C][4]	State Spam Laws	10-54
§ 10:6.4	Sending Automated Text Messages	10-54
§ 10:6.5	Industry Self-Regulation.....	10-55
[A]	Mobile Marketing Association	10-55
[B]	Direct Marketing Association’s Guidelines for Ethical Business Practice.....	10-58
§ 10:7	Social Media	10-59
§ 10:7.1	Source and Scope of Rules.....	10-59
§ 10:7.2	What Is Social Media?	10-60
§ 10:7.3	Sending Commercial Messages via Social Media	10-60

§ 10:7.4	Gathering and Using Consumer Data from Social Media Sites	10-62
[A]	Disclosure of Users' Personal Information to Third Parties.....	10-62
[B]	Address Book Harvesting.....	10-64
[C]	Location-Based Services	10-65
[D]	Computer Fraud Statutes.....	10-65
[E]	Industry Self-Regulation of Information Gathering and Distribution	10-67
§ 10:7.5	Using Social Media Users' Actions As Advertisements	10-68
[A]	Advertising Social Media Users' Activity Within the Social Media Site	10-68
[B]	Advertising Social Media Users' Internet Activity Outside the Social Media Site	10-68
§ 10:7.6	Endorsements Made on Social Media	10-69
§ 10:8	Conclusions.....	10-71

Chapter 11 The Children's Online Privacy Protection Act (COPPA)

Nancy L. Savitt

§ 11:1	Introduction/Overview.....	11-3
§ 11:1.1	Enactment	11-3
§ 11:1.2	Statutory Overview	11-4
§ 11:1.3	Who Enforces the Statute.....	11-5
§ 11:2	Who Is Subject to the Statute	11-6
§ 11:2.1	"Operator"	11-6
[A]	Factors Determining Operator Status	11-9
[B]	Special Cases	11-10
[B][1]	Internet Service Providers and Other "Mere Conduits"	11-10
[B][2]	Advertisers, Plug-Ins, and Related Services.....	11-11
[B][3]	Non-U.S. Operators	11-12
[B][4]	Nonprofits.....	11-13
§ 11:2.2	"Website or Online Service Directed to Children"	11-13
[A]	Primary Content Provider Versus Advertisers and Plug-Ins.....	11-14
[B]	Age-Screening Where Children Are Not "Primary Audience"	11-17
§ 11:2.3	General Audience Website	11-18
[A]	"Actual Knowledge".....	11-19

Table of Contents

§ 11:3	What Activities Does COPPA Cover?	11-20
§ 11:3.1	“Personal Information”	11-20
§ 11:3.2	“Collection”	11-23
[A]	Requesting a Child to Submit Personal Information Online	11-23
[B]	Enabling a Child to Publicly Disclose Personal Information	11-24
[B][1]	To Monitor or Not to Monitor.....	11-25
[C]	Passive Tracking.....	11-25
§ 11:3.3	“Disclosure”.....	11-26
[A]	Release of Personal Information.....	11-26
[A][1]	Third Party Versus Provider of “Support for the Internal Operations of the Website”	11-27
[B]	Making Personal Information Publicly Available	11-29
§ 11:4	How to Comply with COPPA	11-29
§ 11:4.1	Need Prior Parental Consent Unless Fall Within Exception	11-30
[A]	“Verifiable Parental Consent” (“Verifiable Consent”)	11-30
[B]	“Parent”	11-31
[B][1]	Schools.....	11-31
[B][2]	Ascertaining Whether Someone Is a “Parent”	11-32
[B][3]	Parents’ Right to Review and Have Information Deleted.....	11-32
§ 11:4.2	Exceptions to Consent	11-35
[A]	To Obtain Parental Consent.....	11-35
[B]	To Respond to a Child’s Specific Request on a One-Time Basis	11-36
[C]	To Respond More Than Once to a Child’s Specific Request	11-37
[D]	To Protect the Child’s Safety	11-39
[E]	To Protect the Website	11-39
[F]	To Notify and Update Parents About a Website That Does Not Collect Personal Information	11-40
[G]	To Collect a Persistent Identifier in Limited Circumstances	11-40
§ 11:4.3	How to Get Consent.....	11-41
[A]	Notice.....	11-41
[A][1]	Requirements for Notice	11-41
[A][1][a]	“Clear and Understandable”	11-41
[A][1][b]	Information Collected and How It Is Used	11-42
[A][1][c]	Disclosures to Third Parties and Others.....	11-43

[A][1][d]	Parental Review Rights	11-43
[A][1][e]	Operators' Contact Information	11-43
[A][2]	Privacy Policy Placement	11-44
[A][3]	Direct Notice to Parents	11-46
[A][3][a]	“Material Change”	11-46
[B]	Consent	11-47
[B][1]	Full Consent	11-47
[B][1][a]	Print and Send or Scan	11-47
[B][1][b]	Credit Card Transaction	11-47
[B][1][c]	Toll-Free Number or Video Conference	11-48
[B][1][d]	Government-Issued Identification	11-48
[B][1][e]	Other Methods	11-49
[B][2]	Email Plus Consent	11-50
[B][3]	Online Consent Form Insufficient	11-52
§ 11:4.4	What Happens If the Operator Does Not Get Parental Consent	11-52
[A]	Delete Information	11-52
[B]	Limited Permission to Terminate Service	11-53
[B][1]	Cannot Terminate for Non-Consent to Third-Party Disclosure	11-53
§ 11:4.5	Security and Data Retention/Deletion	11-54
§ 11:4.6	Safe Harbors	11-57
§ 11:5	Sanctions/Penalties	11-58
§ 11:5.1	FTC COPPA Enforcement Actions	11-61
§ 11:5.2	FTC Non-COPPA Enforcement	11-65
§ 11:6	State Enforcement Actions	11-66
§ 11:6.1	State of Texas Enforcement Actions	11-66
§ 11:6.2	State of New Jersey Enforcement Actions	11-67
§ 11:6.3	State of New York Enforcement Actions	11-69

Chapter 12 The Privacy Act of 1974 and Its Progeny

Kenneth P. Mortensen & Nuala O'Connor Kelly

§ 12:1	Introduction	12-3
§ 12:2	Privacy Act Statutory Provisions	12-4
§ 12:2.1	5 U.S.C. § 552a(a): Definitions	12-4
[A]	“Agency”	12-4
[A][1]	Privacy Act Applies Only to Federal Agencies	12-4
[A][2]	Executive Office of the President	12-5
[A][3]	State and Local Government Agencies	12-7
[A][4]	Other Entities	12-7
[B]	“Individual”	12-8
[C]	“Maintain”	12-10

Table of Contents

	[D]	“Record”	12-10
	[E]	“System of Records”	12-13
	[F]	“Statistical Record”	12-16
	[G]	“Routine Use”	12-17
§ 12:2.2		5 U.S.C. § 552a(b): Conditions of Disclosure	12-18
	[A]	Disclosure Within Agencies	12-19
	[B]	Disclosure to the Public	12-19
	[C]	Disclosure for a “Routine Use”	12-20
	[D]	Disclosure to the Bureau of the Census	12-22
	[E]	Disclosure for Statistical Research and Reporting	12-23
	[F]	Disclosure to National Archives	12-24
	[G]	Disclosure for Law Enforcement Purposes	12-24
	[H]	Disclosure Under Emergency Circumstances	12-25
	[I]	Disclosure to Congress	12-26
	[J]	Disclosure to the General Accountability Office	12-26
	[K]	Disclosure Pursuant to Court Order	12-26
	[L]	Disclosure to a Consumer Reporting Agency	12-27
	[M]	Disclosure of Social Security Numbers	12-27
§ 12:2.3		5 U.S.C. § 552a(d): Access to Records	12-28
	[A]	Individual Access	12-28
	[B]	Amending Records	12-30
§ 12:2.4		5 U.S.C. § 552a(g)(4): Remedies	12-32
§ 12:3		Systems of Records Notice Guidance	12-32
	§ 12:3.1	Definitions	12-32
	§ 12:3.2	Contents	12-32
	§ 12:3.3	How to Prepare a System of Records Notice	12-33
		[A] Key Elements	12-33
		[B] Storage	12-34
		[C] Record Identification	12-34
		[D] Security Safeguards	12-34
		[E] Retention and Disposal	12-34
		[F] Notification Procedures; Record Access Procedures; Contesting Record Procedures	12-35
		[G] Record Source Categories	12-35
		[H] Systems Exempted from Certain Provisions of the Act	12-35
		[I] Routine Uses	12-36
§ 12:4		E-Government Act Section 208 Statutory Provisions: Privacy Impact Assessments	12-37
	§ 12:4.1	Section 208(b)(1): Responsibilities of Agencies	12-38
		[A] When to Do a Privacy Impact Assessment	12-38
		[B] Agency Activities	12-39
		[C] Sensitive Information	12-39

§ 12:4.2	Section 208(b)(2): Contents of a Privacy Impact Assessment.....	12-40
[A]	OMB Guidance.....	12-40
[B]	What Information Is Collected?.....	12-40
[C]	Why Is the Information Collected?.....	12-41
[D]	What Is the Intended Use of the Information?.....	12-41
[E]	Who Will the Information Be Shared With?.....	12-41
[F]	What Notice Will Be Given Regarding the Information's Use and Collection?.....	12-42
[G]	How Will the Information Be Secured?.....	12-42
[H]	Is a System of Records Notice Created?.....	12-42
§ 12:5	Privacy Impact Assessment Guidance.....	12-42
§ 12:5.1	Introduction.....	12-42
§ 12:5.2	What Is a PIA?.....	12-43
§ 12:5.3	Complying with the PIA Requirement.....	12-43
§ 12:5.4	Information Covered by the PIA.....	12-45
§ 12:5.5	Regarding "Private" Information.....	12-45
§ 12:5.6	Regarding Privacy Act System of Records Notice (SORN) Requirements Versus PIA Requirements.....	12-46
§ 12:5.7	When to Conduct a PIA.....	12-46
§ 12:5.8	Classified Information and Systems.....	12-46
§ 12:5.9	Negative PIAs.....	12-46
§ 12:5.10	How to Conduct a PIA.....	12-46
§ 12:5.11	Writing the PIA.....	12-47
[A]	Introduction.....	12-47
[B]	Section 1.0—The System and the Information Collected and Stored with the System.....	12-48
[C]	Section 2.0—Uses of the System and the Information.....	12-49
[D]	Section 3.0—Retention.....	12-51
[E]	Section 4.0—Internal Sharing and Disclosure.....	12-51
[F]	Section 5.0—External Sharing and Disclosure.....	12-52
[G]	Section 6.0—Notice.....	12-53
[H]	Section 7.0—Individual Access, Redress, and Correction.....	12-54
[I]	Section 8.0—Technical Access and Security.....	12-55
[J]	Section 9.0—Technology.....	12-56
[K]	Conclusion.....	12-56
[L]	Approval and Signature Page.....	12-56

Chapter 13 Canadian Privacy Law

*John Beardwood, Gabriel M.A. Stern &
Anagha Nandakumaran*

§ 13:1	Nature of the Canadian Privacy Framework	13-3
§ 13:1.1	Intersecting Federal and Provincial Privacy Regimes	13-3
[A]	Public Sector	13-4
[B]	Private Sector	13-4
[B][1]	Québec	13-4
[B][2]	Federal	13-6
[B][3]	Provincial (Other Than Québec)	13-7
[C]	Personal Health Information	13-8
[D]	Statutory Tort of Invasion of Privacy	13-9
§ 13:1.2	Privacy Principles from Common Law	13-12
[A]	Common-Law Torts	13-12
[B]	Work Product	13-18
[C]	Surveillance	13-19
[C][1]	Reasonableness of Surveillance in the Workplace	13-19
[C][2]	Surveillance Evidence in Litigation	13-20
[C][3]	Unwanted Surveillance in Public Spaces	13-21
§ 13:1.3	Relationship Between the Canadian and European Privacy Regimes	13-21
§ 13:2	Personal Information	13-25
§ 13:2.1	Scope of Definition of “Personal Information”	13-25
§ 13:2.2	Employee Information	13-25
§ 13:2.3	Carve-Outs from the Obligations Applying to Personal Information	13-26
§ 13:2.4	Sensitivity of Personal Information	13-26
§ 13:3	Nature of Privacy Obligations	13-27
§ 13:3.1	Consent/Notice Obligations	13-27
[A]	Generally	13-27
[B]	Content of the Notice	13-28
[C]	Withdrawing Consent	13-28
[D]	Extra-Jurisdictional Transfers of Personal Information	13-29
§ 13:3.2	Administrative Obligations	13-32
§ 13:3.3	Access Obligations	13-32
§ 13:3.4	Breach Notification	13-33
[A]	Comparison of the Federal and Alberta Models	13-33
[A][1]	Components of the Threshold Test Under PIPEDA	13-34
[A][2]	Components of Threshold Test Under Alberta PIPA	13-35
[A][3]	Responsibility for Notification	13-35

	[A][4]	Third-Party Notifications	13-36
	[A][5]	Recording Obligation.....	13-36
	[A][6]	Offenses	13-36
§ 13:3.5		Enforcement	13-37
	[A]	Generally	13-37
	[B]	Powers	13-37
	[C]	Offenses.....	13-37
	[D]	“Naming and Shaming”	13-38
	[E]	Review of Findings/Appeals.....	13-38
	[F]	Remedies	13-39
§ 13:4		Canadian Privacy Law in Transition	13-39
§ 13:4.1		Overview of the 2015 Amendments to PIPEDA	13-39
	[A]	Valid Consent	13-39
	[B]	Disclosure Consent Exemptions	13-39
	[C]	Collection, Use and Disclosure Exemptions	13-40
	[D]	Business Transaction Provisions	13-40
	[E]	Consent Exemption for Employee Information.....	13-40
	[F]	Complaint Time Period	13-41
	[G]	Compliance Agreement	13-41
	[H]	Privacy Commissioner Right to Publicize	13-41
§ 13:4.2		Proposed 2021 Amendments to PIPEDA Under Bill C-11	13-41
§ 13:4.3		Proposed 2022 Amendments to PIPEDA Under Bill C-27	13-42
	[A]	Consent Requirements	13-42
	[B]	Appropriate Manner and Purposes.....	13-42
	[C]	Exceptions to Consent Requirements: Business Activities and Legitimate Interests.....	13-43
	[C][1]	Business Activities	13-43
	[C][2]	Legitimate Interests.....	13-43
	[D]	Right to Require Disposal of Individual’s Personal Information	13-45
	[E]	Anonymization of Personal Information.....	13-46
	[E][1]	Effects of De-Identification.....	13-46
	[F]	Business Transactions Policies	13-47
	[G]	Enforcement in Bill C-27	13-47
	[G][1]	AMPs	13-47
	[G][2]	Offenses and Fines	13-48
	[G][3]	Private Right of Action	13-48
§ 13:4.4		Law 25; New Amendments to Québec Privacy Legislation	13-48
	[A]	Scope/Application	13-49
	[A][1]	Personal Information.....	13-49
	[A][2]	Organizations Covered by Law 25	13-49
	[A][3]	Consent.....	13-50

Table of Contents

[B]	Privacy Impact Assessments	13-51
[B][1]	PI Project PIA	13-52
[B][2]	PIA for PI Communication/Use Outside Québec	13-52
[B][3]	PI Study PIA	13-53
[C]	Administrative Monetary Penalties	13-53
§ 13:4.5	Canada's Anti-Spam Legislation (CASL)	13-54
§ 13:5	Conclusion	13-54

Chapter 14 International Privacy Laws

Kelly McMullon

§ 14:1	Introduction	14-7
§ 14:2	The GDPR	14-8
§ 14:3	Terminology	14-10
§ 14:4	The Scope of the GDPR	14-11
§ 14:4.1	Material Scope	14-11
§ 14:4.2	Territorial Scope	14-12
[A]	EU-Established Organizations	14-12
[A][1]	Identifying the Data Controller	14-12
[A][2]	Determining the Existence of an "Establishment"	14-13
[A][3]	The Location of the Establishment	14-13
[A][4]	Involvement of Establishment in Activities Relating to Data Processing	14-13
[B]	Non-EU Established Organizations	14-15
[C]	International Law	14-16
§ 14:5	Controllers and Processors	14-16
§ 14:5.1	Controllers	14-17
§ 14:5.2	Processors	14-19
§ 14:5.3	Determining Whether an Entity Is a Controller or Processor	14-20
§ 14:5.4	Joint Controllers	14-20
§ 14:5.5	Data Protection Agreements	14-21
§ 14:5.6	Liability and Sub-Processors	14-22
§ 14:6	Compliance with the GDPR	14-24
§ 14:6.1	Data Protection Principles	14-24
§ 14:6.2	Accountability	14-25
§ 14:6.3	Lawful Basis	14-26
[A]	Consent	14-27
[B]	Legitimate Interests	14-28
[C]	Legal Obligation	14-29
§ 14:6.4	Privacy Policies	14-30
[A]	Purpose of Privacy Policies	14-30
[B]	Content of Privacy Policies	14-30

§ 14:6.5	Data Subject Rights	14-32
§ 14:6.6	Data Protection by Design and by Default	14-34
§ 14:6.7	International Transfers	14-35
[A]	Adequacy Decisions	14-35
[B]	Standard Contractual Clauses	14-37
[B][1]	Standard Contractual Clauses Overview	14-37
[B][2]	<i>Schrems II</i>	14-38
[B][3]	2021 Standard Contractual Clause SCCs.....	14-40
[C]	Binding Corporate Rules	14-43
[C][1]	BCRs Overview	14-43
[C][2]	BCR Requirements	14-43
[C][3]	BCR Application Process	14-47
[D]	Privacy Shield/Data Privacy Framework.....	14-48
[E]	Derogations	14-50
[F]	Additional Transfer Mechanisms	14-51
§ 14:6.8	Data Breaches and Reporting Requirements	14-52
[A]	Data Breaches.....	14-52
[B]	The Reporting Requirements	14-53
[C]	Likelihood and Severity.....	14-55
[D]	Other Breach Notification Obligations	14-57
§ 14:6.9	Data Protection Officer (DPO)	14-57
§ 14:6.10	Data Processing Impact Assessment (DPIA)	14-59
[A]	Obligation to Conduct a DPIA.....	14-60
[B]	Contents of a DPIA	14-60
[C]	Assessment of Risk.....	14-61
§ 14:6.11	Enforcement and Fines	14-62
[A]	Enforcement	14-62
[B]	Fines	14-63
[C]	Notable Action	14-65
§ 14:7	Alternative Approach to Regulating Data Privacy—APEC Privacy Framework	14-65
§ 14:7.1	APEC Cross-Border Privacy Rules	14-66
[A]	Comparison with the EU Data Privacy Model	14-68
§ 14:8	ePrivacy	14-69
§ 14:8.1	Cookies.....	14-69
§ 14:8.2	Data Breach Requirements and Best Practices for ePrivacy	14-75
§ 14:8.3	Direct Marketing	14-75
[A]	Direct Marketing by Email, SMS, MMS, Fax, and Automated Calling.....	14-76
[A][1]	Notification of Purpose	14-76
[A][2]	Prior “Opt-in” Consent.....	14-77
[A][3]	Right to Opt Out.....	14-78
[B]	Non-Automated (“Person to Person”) Telephone Marketing	14-78
[C]	Postal Direct Marketing.....	14-79

Table of Contents

§ 14:9	Employee Privacy.....	14-79
§ 14:9.1	Monitoring of Employees.....	14-79
§ 14:9.2	Diversity Initiatives.....	14-81
§ 14:9.3	Investigations and Discovery.....	14-82
§ 14:9.4	Background Screening.....	14-83
§ 14:9.5	Company Intranet.....	14-84
§ 14:9.6	Human Resource Information Systems.....	14-85
§ 14:10	Country Summaries.....	14-86
§ 14:10.1	Europe (European Union).....	14-86
[A]	Belgium.....	14-86
[A][1]	The Local Legal Landscape.....	14-86
[A][2]	Enforcement.....	14-87
[A][3]	Competences and Powers.....	14-87
[A][4]	Guidance.....	14-88
[A][5]	Registrations and Pre-Authorizations.....	14-89
[A][6]	Key Differences.....	14-89
[B]	France.....	14-91
[B][1]	The Local Legal Landscape.....	14-91
[B][2]	Enforcement.....	14-92
[B][3]	Competences and Powers.....	14-96
[B][4]	Guidance.....	14-96
[B][5]	Registrations and Pre-Authorizations.....	14-98
[B][6]	Key Differences.....	14-99
[C]	Germany.....	14-99
[C][1]	The Local Landscape.....	14-99
[C][2]	Enforcement.....	14-99
[C][3]	GDPR Guidance.....	14-100
[C][4]	Key Differences.....	14-100
[D]	Poland.....	14-101
[D][1]	The Local Landscape.....	14-101
[D][2]	Enforcement.....	14-101
[D][3]	Key Differences.....	14-101
[E]	Spain.....	14-103
[E][1]	The Local Landscape.....	14-103
[E][2]	Enforcement.....	14-103
[E][3]	GDPR Guidance.....	14-104
§ 14:10.2	Europe (Non-European Union).....	14-105
[A]	UK.....	14-105
[A][1]	The Local Landscape.....	14-105
[A][2]	Enforcement.....	14-105
[A][3]	UK GDPR Guidance.....	14-106
[A][4]	Registrations and Pre-Authorizations.....	14-108
[A][5]	Data Transfers.....	14-109
[A][6]	Proposed Reforms to UK GDPR.....	14-109

	[B]	Switzerland.....	14-110
	[B][1]	Overview.....	14-110
	[B][2]	Personal Data.....	14-111
	[B][3]	Restrictions on Processing of Personal Data	14-111
	[B][4]	Transfer and Disclosure.....	14-112
	[B][5]	Sensitive Personal Data and High-Risk Profiling.....	14-114
	[B][6]	Enforcement.....	14-115
	[B][7]	Recent Developments.....	14-117
§ 14:10.3		Asia/Pacific.....	14-119
	[A]	Mainland China	14-119
	[A][1]	Overview.....	14-119
	[A][2]	Personal Information.....	14-121
	[A][3]	Collection and Processing.....	14-121
	[A][4]	Storage and Security.....	14-123
	[A][5]	Data Localization and Cross-Border Transfer.....	14-124
	[A][6]	Enforcement.....	14-125
	[A][7]	Recent Developments.....	14-125
	[B]	Hong Kong.....	14-126
	[B][1]	Overview.....	14-126
	[B][2]	Personal Data.....	14-127
	[B][3]	Restrictions on Processing and Use	14-127
	[B][4]	Transfer and Disclosure.....	14-128
	[B][5]	Enforcement.....	14-129
	[B][6]	Data Breach Notification.....	14-129
	[B][7]	Direct Marketing.....	14-130
	[B][8]	Recent Developments.....	14-130
	[C]	India.....	14-131
	[C][1]	Overview.....	14-131
	[C][2]	Personal and Sensitive Data	14-133
	[C][3]	Restrictions on Processing and Use	14-135
	[C][4]	Transfer and Disclosure.....	14-139
	[C][5]	Rights and Duties of Data Principals.....	14-140
	[C][6]	Exemptions Under the DPDP Act.....	14-142
	[C][7]	Enforcement.....	14-143
	[C][8]	Data Breach Notification.....	14-145
	[C][9]	Recent Developments.....	14-146
	[D]	Japan	14-147
	[D][1]	Overview.....	14-147
	[D][2]	Personal Information.....	14-148
	[D][3]	Restrictions on Processing and Use	14-149
	[D][4]	Transfer and Disclosure.....	14-149
	[D][5]	Sensitive Data	14-149
	[D][6]	Enforcement.....	14-150

Table of Contents

[E]	Philippines.....	14-150
[E][1]	Overview.....	14-150
[E][2]	Personal Information.....	14-153
[E][3]	Restrictions on Processing and Use.....	14-153
[E][4]	Transfer and Disclosure.....	14-155
[E][5]	Sensitive Data.....	14-156
[E][6]	Enforcement.....	14-158
[F]	Singapore.....	14-161
[F][1]	Overview.....	14-161
[F][2]	Personal Information.....	14-161
[F][3]	Restrictions on Processing and Use.....	14-161
[F][4]	Transfer and Disclosure.....	14-163
[F][5]	Sensitive Data.....	14-164
[F][6]	Enforcement.....	14-164
[F][7]	Mandatory Data Breach Notification.....	14-165
[F][8]	Recent Developments.....	14-165
[G]	Taiwan.....	14-168
[G][1]	Overview.....	14-168
[G][2]	Personal Information.....	14-169
[G][3]	Restrictions on Collection, Processing, and Use.....	14-169
[G][4]	Transfer and Disclosure.....	14-171
[G][5]	Sensitive Information.....	14-172
[G][6]	Enforcement.....	14-173
[H]	Vietnam.....	14-175
[H][1]	Overview.....	14-175
[H][2]	Personal Information.....	14-178
[H][3]	Restrictions on Processing and Use.....	14-179
[H][4]	Transfer and Disclosure.....	14-181
[H][5]	Sensitive Data.....	14-182
[H][6]	Enforcement.....	14-183
[H][7]	Data Breach Notification.....	14-187
§ 14:10.4	Latin America.....	14-188
[A]	Argentina.....	14-188
[A][1]	Overview.....	14-188
[A][2]	Restrictions on Processing and Use.....	14-189
[A][3]	Transfer and Disclosure.....	14-190
[A][4]	Sensitive Data.....	14-192
[A][5]	Enforcement.....	14-193
[A][6]	Data Breach Notification.....	14-194
[A][7]	Recent Developments.....	14-195
[A][8]	Data Protection Bill.....	14-196
[B]	Brazil.....	14-197
[B][1]	Overview.....	14-197
[B][2]	Personal Data.....	14-198

[B][3]	Enforcement.....	14-199
[B][4]	Data Breach Notification.....	14-200
[B][5]	Recent Developments.....	14-201
§ 14:10.5	Africa and the Middle East.....	14-201
[A]	Israel.....	14-201
[A][1]	Overview.....	14-201
[A][2]	Personal and Sensitive Data.....	14-203
[A][3]	Restrictions on Processing and Use.....	14-204
[A][4]	Transfer and Disclosure.....	14-204
[A][5]	Enforcement.....	14-207
[A][6]	Recent Developments.....	14-209
[A][6][a]	Amendment Proposal for the Protection of Privacy Law.....	14-209
[A][6][b]	Independence of the Privacy Protection Authority.....	14-210
[A][6][c]	New Regulations Regarding Data Transfer from the EEA.....	14-210
[B]	Oman.....	14-211
[B][1]	Overview.....	14-211
[B][2]	Personal Data.....	14-211
[B][3]	Restrictions on Processing and Use.....	14-212
[B][4]	Transfer and Disclosure.....	14-214
[B][5]	Data Breach Notification.....	14-214
[B][6]	Enforcement.....	14-215
[B][7]	Recent Developments.....	14-215
[C]	Qatar.....	14-215
[C][1]	Local Landscape/Overview.....	14-215
[C][2]	Personal Information.....	14-216
[C][3]	Restrictions on Processing and Use.....	14-216
[C][4]	Transfer and Disclosure.....	14-221
[C][5]	Enforcement.....	14-223
[C][6]	Recent Developments.....	14-223
[D]	Saudi Arabia.....	14-224
[D][1]	Overview.....	14-224
[D][2]	Personal Information.....	14-225
[D][3]	Restrictions on Processing and Use.....	14-225
[D][4]	Transfer and Disclosure.....	14-227
[D][5]	Sensitive Data.....	14-228
[D][6]	Enforcement.....	14-228
[D][7]	Data Breach Notification.....	14-229
[E]	United Arab Emirates.....	14-230
[E][1]	Overview.....	14-230
[E][1][a]	UAE.....	14-230
[E][1][b]	DIFC.....	14-231
[E][1][c]	ADGM.....	14-232

Table of Contents

[E][2]	Personal Information.....	14-232
[E][2][a]	UAE	14-232
[E][2][b]	DIFC	14-233
[E][2][c]	ADGM	14-233
[E][3]	Restrictions on Processing and Use	14-233
[E][3][a]	UAE	14-233
[E][3][b]	DIFC	14-234
[E][3][c]	ADGM	14-235
[E][4]	Transfer and Disclosure.....	14-237
[E][4][a]	UAE	14-237
[E][4][b]	DIFC	14-238
[E][4][c]	ADGM	14-239
[E][5]	Sensitive Data	14-240
[E][5][a]	UAE	14-240
[E][5][b]	DIFC	14-240
[E][5][c]	ADGM	14-241
[E][6]	Enforcement.....	14-241
[E][6][a]	UAE	14-241
[E][6][b]	DIFC	14-242
[E][6][c]	ADGM	14-243
[E][7]	Data Breach Notification.....	14-243
[E][7][a]	UAE	14-243
[E][7][b]	DIFC	14-244
[E][7][c]	ADGM	14-245

Chapter 15 Compliance with the Payment Card Industry Data Security Standard

Mark MacCarthy, Pieter Penning & David Ames

§ 15:1	Introduction	15-2
§ 15:2	Background.....	15-6
§ 15:2.1	Industry Background.....	15-6
§ 15:2.2	Federal Consumer Protection Laws	15-9
§ 15:2.3	Data Security Regulations.....	15-10
[A]	Federal Regulation	15-10
[B]	State Regulation.....	15-12
§ 15:3	Development of the Payment Card Industry Data Security Standard.....	15-13
§ 15:4	PCI Requirements	15-19
§ 15:4.1	The Basic Requirements	15-19
Figure 15-1	Payment Card Industry Data Security Standard....	15-20
§ 15:4.2	Protecting Stored Data	15-24
Figure 15-2	PCI Requirement 3: Protect Stored Cardholder Data.....	15-24

§ 15:4.3	Encrypt Transmission of Cardholder Data Across Open, Public Networks.....	15-29
Figure 15-3	Requirement 4: Encrypt Transmitted Data	15-30
§ 15:4.4	Compensating Controls.....	15-31
§ 15:4.5	Payment Applications	15-31
§ 15:5	Validation	15-33
§ 15:5.1	Merchant Levels	15-35
Figure 15-4	Merchant Levels (Visa CISP).....	15-36
§ 15:5.2	Service Provider Levels.....	15-36
Figure 15-5	Service Provider Levels (Visa CISP)	15-37
§ 15:5.3	Merchant Validation Requirements.....	15-38
Figure 15-6	Merchant Levels and Validation Requirements (Visa CISP).....	15-38
§ 15:5.4	Service Provider Validation Requirements	15-39
Figure 15-7	Service Provider Levels and Validation Requirements (Visa CISP).....	15-40
§ 15:5.5	Corporate Franchise Servicers	15-40
§ 15:6	After a Compromise	15-42
§ 15:6.1	Background.....	15-42
§ 15:6.2	Initial Steps.....	15-44
§ 15:6.3	Monitoring At-Risk Accounts	15-47
§ 15:6.4	Notification to Issuing Financial Institutions	15-48
§ 15:7	Enforcement	15-50
§ 15:7.1	General.....	15-50
§ 15:7.2	Enforcement Efforts	15-51
§ 15:7.3	CardSystems Solutions	15-53
§ 15:7.4	Other Significant Data Breaches	15-54
§ 15:8	Continued Development of Cardholder Data Protection	15-56
§ 15:8.1	Increasing Global Compliance	15-56
§ 15:8.2	Chip and PIN Security	15-57
§ 15:8.3	Tokenization	15-60
§ 15:8.4	Point-to-Point Encryption	15-61
§ 15:8.5	Mobile Payments	15-61
§ 15:8.6	Cloud Computing.....	15-63
§ 15:8.7	E-Commerce.....	15-64
§ 15:8.8	Risk Assessments	15-65

**Chapter 16 Insurance for Data Breaches, Cyber Crime, and
Unauthorized Privacy Disclosures**

Steven R. Gilford & Marc E. Rosenthal

§ 16:1	Overview	16-2
§ 16:2	Applicability of Historic Coverages	16-6

Table of Contents

§ 16:2.1	First- and Third-Party Coverages for Property Loss	16-7
[A]	First-Party Property Policies	16-8
[B]	Third-Party CGL Policies: Coverage for Property Damage Claims	16-11
§ 16:2.2	CGL Coverage for Personal and Advertising Injury Claims	16-14
[A]	Publication Requirement	16-16
[B]	Right to Privacy As an Enumerated Offense.....	16-20
[B][1]	Telephone Consumer Protection Act Cases	16-23
[B][2]	Biometric Information Cases	16-28
[B][3]	ZIP Code, Credit Card, and Other Statutes.....	16-33
§ 16:2.3	Other Coverages	16-35
[A]	Directors and Officers Liability Insurance.....	16-35
[B]	Errors and Omission Policies	16-37
[C]	Crime Policies.....	16-40
§ 16:3	Modern Cyber Policies.....	16-45
§ 16:3.1	Key Concepts in Cyber Coverage	16-47
[A]	Named Peril.....	16-47
[B]	Claims Made	16-49
§ 16:3.2	Issues of Concern in Evaluating Cyber Risk Policies.....	16-51
[A]	What Is Covered?	16-51
[B]	Confidential Information, Privacy Breach, and Other Key Definitions.....	16-52
[C]	Overlap with Existing Coverage	16-53
[D]	Limits and Deductibles.....	16-54
[E]	Notice Requirements	16-55
[F]	Coverage for Regulatory Investigations or Actions	16-57
[G]	Definition of Loss	16-64
[H]	Who Controls Defense and Settlement.....	16-67
[I]	Control of Public Relations and Crisis Management Professionals	16-72
[J]	Issues Created by Involvement of Policyholder Employees.....	16-73
[K]	Coverage of a <i>Threatened</i> Security Breach— Ransomware	16-77
[L]	Coverage for “Breachless” Claims	16-79
[M]	The “Internet of Things” and Potential Physical Damage or Bodily Injury from a Cyber Attack.....	16-81
[N]	Governmental Activity Exclusion	16-84
[O]	Other Exclusions	16-87
§ 16:3.3	SEC Disclosure and Other Regulatory Initiatives.....	16-91

Chapter 17 Data Breach Litigation

Margaret A. Dale & David A. Munkittrick

§ 17:1 Introduction 17-2

§ 17:2 Consumer Plaintiff Theories of Liability..... 17-2

 § 17:2.1 Causes of Action..... 17-2

 [A] Negligence 17-3

 [B] Breach of Contract..... 17-3

 [C] Fraud 17-4

 § 17:2.2 Actual Damages..... 17-4

§ 17:3 Defense Strategies 17-4

 § 17:3.1 Standing..... 17-4

 [A] The Supreme Court on Standing 17-4

 [B] Data Breach Standing in Circuit Courts of Appeals..... 17-8

 [B][1] First Circuit..... 17-9

 [B][2] Second Circuit..... 17-10

 [B][3] Third Circuit..... 17-12

 [B][4] Fourth Circuit 17-13

 [B][5] Sixth Circuit..... 17-14

 [B][6] Seventh Circuit 17-14

 [B][7] Eighth Circuit 17-16

 [B][8] Ninth Circuit 17-16

 [B][9] Eleventh Circuit 17-17

 [B][10] D.C. Circuit..... 17-18

 [C] Standing Decisions in U.S. District Courts 17-19

 § 17:3.2 Failure to State a Claim upon Which Relief Can Be Granted (Rule 12(b)(6)) 17-24

 § 17:3.3 Motions to Compel Arbitration 17-28

 § 17:3.4 Surviving Discovery 17-31

 § 17:3.5 Surviving Other Motions 17-32

 [A] Motions for Summary Judgment 17-32

 [B] Motions for Class Certification..... 17-34

§ 17:4 Non-Consumer Plaintiffs 17-41

 § 17:4.1 Shareholder Derivative Suits..... 17-41

 § 17:4.2 Attorney General Suits..... 17-42

 § 17:4.3 Securities Suits 17-43

 § 17:4.4 Claims Brought by Financial Institutions 17-48

§ 17:5 Noteworthy Settlements..... 17-51

Chapter 18 Location Privacy: Technology and the Law

David A. Munkittrick

§ 18:1 Introduction 18-2

§ 18:2 Development and Uses of Location-Tracking Technologies 18-2

 § 18:2.1 Overview..... 18-2

 § 18:2.2 Global Positioning Systems..... 18-3

 § 18:2.3 Cell Site Location Information..... 18-6

 § 18:2.4 Indoor Positioning Systems..... 18-8

 [A] Radio Frequency Identification 18-8

 [B] Other IPS Technologies..... 18-9

 § 18:2.5 Vehicle Tracking..... 18-10

 § 18:2.6 Unmanned Drones 18-12

§ 18:3 Government Collection of Location Information..... 18-12

 § 18:3.1 Location Privacy Under the Fourth Amendment..... 18-12

 § 18:3.2 Government Requests for CSLI 18-16

 [A] Federal Statutes 18-16

 [B] Case Law 18-18

 [C] State Laws..... 18-27

§ 18:4 Private Collection and Use of Location Information 18-28

 § 18:4.1 GPS Tracking..... 18-28

 [A] State Laws..... 18-28

 [B] Case Law 18-29

 [C] Industry Self-Regulation 18-32

 § 18:4.2 Mobile Devices and Applications 18-33

 [A] Agency Guidance 18-33

 [B] Litigation 18-35

 § 18:4.3 Other Location Technologies..... 18-42

 [A] Radio Frequency Identification 18-42

 [B] Vehicle Tracking..... 18-43

 [C] Unmanned Drones 18-45

Index I-1

